IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

INSTALLATION SOFTWARE TECHNOLOGIES, INC. d/b/a INSTALLSHIELD SOFTWARE CORPORATION,

Plaintiff,

v.

WISE SOLUTIONS, INC.,

Defendant.

Civil Action No. 03 C 4502

Hon. David H. Coar
Presiding Judge
Hon. Morton Denlow
Magistrate Judge

NOTICE OF FILING

TO: Michael J. Abernathy
Scott M. Mendel
Lisa A. Carroll
Bell Boyd & Lloyd LLC
Three First National Plaza
Suite 3300
Chicago, IL 60602

PLEASE TAKE NOTICE that on the 3rd day of December, 2003, we filed with the Clerk of the United States District Court, Northern District of Illinois, Eastern Division, Plaintiff, InstallShield's Corrected Memorandum in Opposition to Defendant Wise Solutions, Inc.'s Motion for Partial Summary Judgment, a copy of which is attached hereto.

One of the Attorneys for Plaintiff, Installation Software Technologies, d/b/a InstallShield Software Corporation

William Lynch Schaller
John M. Murphy
Charles R. Topping
Hillary P. Krantz
BAKER & McKENZIE
One Prudential Plaza
130 East Randolph Drive
Chicago, IL 60601
(312) 861-8000
Firm ID: 28

39

CERTIFICATE OF SERVICE

I hereby certify that (1) I am an attorney admitted to appear before this Court and (2) I caused true and correct copies of the foregoing Notice of Filing, Plaintiff InstallShield's Corrected Memorandum in Opposition to Defendant Wise Solutions, Inc.'s Motion for Partial Summary Judgment to be sent to the following individual:

Michael J. Abernathy
Bell Boyd & Lloyd LLC
Three First National Plaza
Suite 3300
Chicago, IL 60602

by first class mail this 3rd day of December 2003.

One of the Attorneys for Plaintiff,
Installation Software Technologies, d/b/a
Installshield Software Corporation

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

INSTALLATION SOFTWARE TECHNOLOGIES, INC. d/b/a INSTALLSHIELD SOFTWARE CORPORATION,)
Plaintiff,)
v.) No. 03 C 4502
WISE SOLUTIONS, INC.,) Judge Coar
Defendant.) Magistrate Judge Denlow

PLAINTIFF INSTALLSHIELD'S CORRECTED MEMORANDUM IN OPPOSITION TO DEFENDANT WISE SOLUTIONS, INC.'S MOTION FOR PARTIAL SUMMARY JUDGMENT

Plaintiff, Installation Software Technologies, Inc. d/b/a InstallShield Software Corporation (hereinafter "InstallShield"), for its Memorandum in Opposition to Defendant Wise Solutions, Inc.'s (hereinafter "Wise") Motion for Partial Summary Judgment, states the following:

I. INTRODUCTION

As the sole basis for Wise's motion for partial summary judgment as to Count IV of InstallShield's Verified Complaint, Wise argues that InstallShield's trade secrets were not "the subject of efforts that [were] reasonable under the circumstances to maintain [their] secrecy or confidentiality," as required by Section 2(d) of the Illinois Trade Secrets Act ("ITSA"), 765 ILCS 1065/1 *et seq.* The crux of Wise's summary judgment argument is that irrespective of the nature and scope of InstallShield's secrecy efforts, InstallShield forfeited its trade secret protection when it placed files containing the trade secrets at issue in the outgoing folder of its ftp server, where access to them could be obtained by typing in the password, "anonymous."

39

Wise's summary judgment papers suffer from two glaring omissions, one procedural and one substantive. First, Wise nowhere cites *Rockwell Graphics Systems, Inc. v. DEV Industries, Inc.*, 925 F.2d 174 (7th Cir. 1991), even though *Rockwell Graphics* constitutes the controlling procedural precedent on this summary judgment motion. Second, Wise nowhere cites a computer password case, much less one granting summary judgment on the sole ground that use of an unsophisticated computer password, in the context of otherwise elaborate security measures, renders the entire security scheme unreasonable as a matter of law under the ITSA. Wise's omissions are unsurprising: *Rockwell Graphics* sets an extraordinarily high summary judgment standard for a defendant whose only argument is an attack on reasonable secrecy measures, and everyone knows it is a federal crime to hack into a password-protected computer system, no matter how weak or strong the passwords may be. "The maintenance of standards of commercial ethics," the very purpose of trade secret law, requires that Wise's motion be denied. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974); *Brunswick Corp. v. Outboard Marine Corp*, 79 Ill.2d 475, 478, 404 N.E.2d 205, 207, 38 Ill. Dec. 781 (1980).

II. STATEMENT OF FACTS

From July 1, 2002 to June 23, 2003 defendant Wise repeatedly and systematically broke into InstallShield's ftp server on 837 occasions.[1] PSAMF, ¶¶ 51-56. Using the confidential usernames and passwords of two InstallShield employees, Wise downloaded 706 files without InstallShield's knowledge or authorization. PSAMF, ¶ 55. Also, without InstallShield's knowledge or authorization, Wise downloaded 197 additional files from InstallShield's ftp server using the username "anonymous." PSAMF, ¶ 55. Wise's extraordinary misconduct is the subject

[1] As used herein, "PSAMF" refers to Plaintiff's Statement of Additional Material Facts submitted by plaintiff pursuant to Local Rule 56.1(b)(3)(B). For example, "PSAMF, ¶¶ 51-56 refers to Paragraphs 51-56 of Plaintiff's Statement of Additional Material Facts.

of an ongoing criminal investigation by the Federal Bureau of Investigation and the United States Attorney for the Northern District of Illinois.

Among the 903 files taken by Wise were four files containing InstallShield's trade secrets: (1) a file containing the names, addresses and contact information for approximately 103,000 InstallShield customers ("the 103,000 Customer List"); (2) a file containing the names, addresses and specific contact information of 6,000 customers interested in InstallShield's AdminStudio software product ("the 6,000 Customer List"); (3) a file containing the concept advertising copy and artwork for InstallShield's advertising campaign, "Cast Your Net Far and Wide"; and (4) InstallShield's beta software for its AdminStudio 5.0 product. PSAMF ¶¶ 58, 62, 63, 67, 93, 97, 105, 120.

III. ARGUMENT

A. Controlling Seventh Circuit Precedent

The Court of Appeals in *Rockwell Graphics* squarely set forth the procedural standards that govern the summary judgment motion before this Court:

> But only in an extreme case can what is a 'reasonable' precaution be determined on a motion for summary judgment, because the answer depends on a balancing of costs and benefits that will vary from case to case and require estimation and measurement by persons knowledgeable in the particular field of endeavor involved.
>
> * * *
>
> There are contested factual issues here, bearing in mind that what is reasonable is itself a fact for purposes of Rule 56 of the Civil Rules.

925 F.2d at 179-80, *citing Cooter & Gell v. Hartmarx Corp.*, 496 U.S. 384 (1990) and *Mucha v. King*, 792 F.2d 602, 605 (7th Cir. 1986).

The Court of Appeals has provided ample guidance as to when the reasonableness of secrecy measures constitutes a question of fact. In *Rockwell Graphics*, the Court of Appeals held that stamping drawings with confidentiality legends, maintaining drawings in a vault, and using sign-in/sign-out procedures constituted sufficient secrecy measures to withstand summary judgment – even though Rockwell did not limit copying of its drawings and did not insist that copies be returned, resulting in "tens of thousands of copies of these drawings...floating around outside Rockwell's vault, and many of these outside the company altogether." 925 F.2d at 177. Similarly, in *Mangren Research and Development Corp. v. National Chemical Co., Inc.*, 87 F.3d 937, 943 (7th Cir. 1996), the Court of Appeals, relying upon *Rockwell*, held that a question of fact existed as to the reasonableness of secrecy efforts used to guard chemical ingredients for a mold release formula – even though "a devious potential competitor" could have ascertained the relevant ingredients by reading labels on chemicals delivered to the dock at plaintiff's premises. More recently, in *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 725 (7th Cir. 2003), a trade secret/idea theft case, the Court of Appeals held that whether use of an oral confidentiality agreement constituted reasonable secrecy measures was a question of fact for the jury, emphasizing that the ITSA "does not require perfection."

B. InstallShield Used Reasonable Secrecy Measures

InstallShield has employed affirmative secrecy measures that have been deemed sufficient in other cases. *See RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 874-75 (N.D. Ill. 2001) (finding that disclosure to employees on a "need-to-know" basis, password-protected computer databases and employee confidentiality agreements were sufficient to constitute reasonable efforts to protect confidential customer information under the ITSA). For example:

- As a condition of employment, each of InstallShield's employees agrees to maintain in strict confidence InstallShield's proprietary information, including "computer programs and databases ... client lists ... [and] marketing plans and strategies," and to "comply with and abide by security policies and procedures implemented from time to time by InstallShield including...those specifying measures to be taken to safeguard the confidentiality of inventions, trade secrets, confidential knowledge and proprietary information of InstallShield." PSAMF, ¶¶ 9-11.

- InstallShield employs an electronic keycard entry system and monitors its entrance to its premises through video surveillance. PSAMF, ¶¶ 4-8.

- InstallShield's ftp server is placed in a DMZ, has a firewall to prevent access by hackers, and regularly receives Microsoft "patches" to address vulnerabilities to computer crime. PSAMF, ¶¶ 24-26 The local administrator password for the ftp server is known only by three InstallShield employees and is usually changed on a quarterly basis. PSAMF, ¶¶ 21-22.

- InstallShield has never advertised or published on its public internet website, www.installshield.com, the fact that it maintains an ftp server. PSAMF, ¶ 27.

- InstallShield restricts access to its customer mailing lists, including the 103,000 Customer List and the 6,000 Customer List, to employees with a "need to know," and requires employees to maintain the mailing lists in confidence. PSAMF, ¶¶ 68-69 InstallShield's customer list is not provided to third parties either for sale or use. PSAMF, ¶ 70. InstallShield had an agreement with its direct mail printing vendor to maintain the 103,000 Customer List and the 6,000 Customer List in strict confidence. PSAMF, ¶ 72. InstallShield's direct mail printing vendor maintained InstallShield's mailing lists in strict confidence, and requires its employees to maintain this information in strict confidence. PSAMF, ¶¶ 73-75. InstallShield uses "decoys" in its mailing lists to monitor unauthorized use or disclosure. PSAMF, ¶¶ 85-90.

- Both the 103,000 Customer Mailing List and the 6000 Customer Mailing List are generated from InstallShield's CRM Tool. MSAMF ¶ 77. InstallShield's CRM Tool prohibits access to customer information to those who do not have authentication through InstallShield's computer network and restricts access to only authorized employees and contractors. PMSAF, ¶ 79. To assist in restricting access to the CRM Tool to only the individuals and contractors who have been authorized by InstallShield to do so, authorized employees and contactors are issued confidential usernames and passwords for this purpose. PMSAF, ¶ 80. Upon the termination of employment or contractor status of an individual authorized to access the CRM Tool, the individual's username and password are cancelled. PMSAF, ¶ 81. InstallShield authorized only four individuals in its organization to perform maintenance on its CRM Tool (only three prior to March 31, 2003). PMSAF, ¶ 83.

- Only members of InstallShield's marketing department and senior management were given access to the advertising concept, copy and artwork for its "Cast Your Net Far and Wide" advertising campaign. PSAMF, ¶ 98. This information was not disclosed to outside parties, other than to the publisher of the periodical in which the advertising appeared. PSAMF, ¶ 99. InstallShield and the publisher had an understanding that InstallShield's advertising would be treated confidentially prior to publication. PSAMF, ¶ 99.

- InstallShield's Beta Software for AdminStudio 5.0 was provided to 32 customers and prospects, each of which agreed to the terms of an End User License Agreement preventing the recipient from demonstrating or showing the Beta Software to third parties. PSAMF ¶¶ 105, 108. The Beta Software was password-protected such that it could not be installed or operated without a unique password disclosed to each of the 32 recipients. PSAMF ¶¶ 106, 107. InstallShield carefully screens and performs a background check on candidates for positions in InstallShield's software development department. PSAMF, ¶ 101.

- The incoming folder of InstallShield's ftp server is password-protected such that no person may view the contents of or download files placed in the incoming folder, unless that person has a confidential username and password supplied by InstallShield. PSAMF, ¶ 28. Files placed in the incoming folder are also password-protected; one could use a confidential username and password supplied by InstallShield, or alternatively, one could use the username, "anonymous." PSAMF, ¶¶ 29-30.

- InstallShield employees who are provided with access to files placed on InstallShield's ftp server to perform their employment responsibilities are provided with confidential usernames and passwords permitting such access. (PSAMF, ¶ 32). Upon termination of employment, an employee's confidential password is cancelled. (PSAMF, ¶ 34). InstallShield's passwords consist of computer-generated random series of characters, and are not ascertainable through speculation or guesswork. (PSAMF, ¶ 34). InstallShield is not aware of any instance in which an employee disclosed his or her confidential username and password to an external third party. (PSAMF, ¶ 35).

- InstallShield's employees were instructed not to place a file containing confidential or proprietary information in the outgoing folder without first applying a password unique to the file. PSAMF, ¶ 20. This policy is contained in InstallShield's "FTP Server Administration Policy." PSAMF, ¶¶ 36-38. Employees read and sign InstallShield's FTP Server Administration Policy before receiving passwords that afford access to files placed in incoming and outgoing folders of the ftp server. PSAMF, ¶ 36. As set forth in InstallShield's FTP Server Administration Policy, before placing confidential or proprietary information in the outgoing file of the ftp server, every employee is required to verify "that a strong password (10 chars minimum) and unlocking code is applied & is correct (if required) and that the password is NEVER placed on the same SERVER as the locked file to which it pertains." PSAMF, ¶ 39.

- It was also InstallShield's policy and practice to remove confidential information placed by InstallShield in the outgoing folder of its ftp server after the information is obtained by a customer or vendor with authorized access to the ftp server. (PSAMF, ¶ 46). It is also InstallShield's practice to periodically purge all of the files on its ftp server, regardless of whether such files contain confidential information. (PSAMF, ¶ 47). InstallShield periodically reminds employees of this policy and practice both orally and in writing. (PSAMF, ¶ 48).

- As also set forth in InstallShield's FTP Server Administration Policy, before placing information on the ftp server, every InstallShield employee is required to (1) verify that the "virus checker has an UP-TO-DATE virus signature file (*i.e.*, the date of the upload) and has found no contaminated files," (2) he has "uploaded all files to the correct server, in the correct designation with [his or her] login Username and password," (3) that he will "remove all files uploaded in [his or her] Username in a timely fashion …," (4) that he would "not allow any other person to use [his or her] access rights to the FTP SERVER without the Systems' Dept. consent," that "the exact contents of all files to be uploaded," and (5) that he is responsible for complying with the FTP Server Administration Policy and that "to do otherwise may compromise [InstallShield's] file security and thereby jeopardize [InstallShield's] competitive position in the industry." PSAMF, ¶ 40-46.

- Upon discovering Wise's access to its trade secrets, InstallShield promptly took action by promptly investigating Wise's access to its ftp server, by bringing this lawsuit, by reporting Wise's actions to proper authorities, and by seeking a temporary restraining order and preliminary injunction to prevent the further use and disclosure of its trade secrets. PSAMF, ¶¶ 123-32.

It is undisputed that without InstallShield's knowledge or authorization, Wise acquired access to and downloaded the 103,000 Customer List and InstallShield's copying artwork for its advertising campaign using the confidential username and password of InstallShield employee, Jill Kawell. PSAMF ¶¶ 62, 97. It is also undisputed that Wise obtained access to and downloaded the 6,000 Customer List and Wise's Beta Software using the username, "anonymous." PSAMF ¶¶ 67, 120. Of these files, only the Beta Software file had an additional layer of password protection as contemplated by InstallShield's FTP Server Administration Policy. PSAMF ¶¶ 106, 107, 122.

C. InstallShield Did Not Have To Do More To Protect Against Criminal Hackers

Wise's position, in essence, is that InstallShield could have done more to fend off criminal hackers like Wise. Implicit in Wise's view, of course, is that unsophisticated password protection constitutes an invitation to hack into a computer system to steal business data for competitive purposes. But courts have taken a very different view of passwords, properly recognizing that computer access restrictions signify a computer system owner's warning to others of its property rights. *Cf. Muick v. Glenayre Electronics*, 280 F.3d 755 (7th Cir. 2002) (company's computer access and inspection policies placed employees on notice that they had no legal rights with respect to company's computer data). Indeed, courts have gone much further, routinely holding that conduct such as Wise's constitutes trespass, and criminal trespass at that. *See United States v. Seidlitz*, 589 F.2d 152, 160 (4th Cir. 1978) ("In this sense the use by the witnesses below of the term "intruder" to describe an unauthorized user of the computers is aptly applied to the defendant, since by telephonic signal he in fact intruded or trespassed upon the physical property of OSI as effectively as if he had broken into the Rockville facility and instructed the computers from one of the terminals directly wired to the machines"); *State Wide PhotoCopy Corp. v. Tokai Financial Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (defining computer hackers as "electronic trespassers"); *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1567, 54 Cal. Rptr. 2d 468, 473 (4th Dist. 1996) (equating computer hackers with criminal trespassers). Such holdings are simply common sense: everyone today knows it is a federal crime to knowingly obtain unauthorized access to a computer and to circumvent password protection, which is precisely why Wise is presently under criminal investigation by the Federal Bureau of Investigation and the United States Attorney for the Northern District of Illinois. *See* Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030 *et seq.* and Digital Millennium Copyright Act, 17 U.S.C. §§ 1201 *et seq.*

Any computer password, no matter how unsophisticated, constitutes constructive notice that authorization is required before entry is permitted. *See Specht v. Netscape Communications Corp.*, 306 F.3d 17, 30, n.14 (2d Cir. 2002) ("Inquiry notice is actual notice of circumstances sufficient to put a prudent man upon inquiry."), *quoting Cal State Auto. Ass'n Inter-Ins. Bureau v. Barrett Garages, Inc.*, 257 Cal. App. 2d 71, 77, 64 Cal. Rptr. 699, 703 (Cal. Ct. App. 1967). The reason the law requires reasonable secrecy measures is not to prevent criminal attacks, but rather "to apprise employees of the claim of secrecy and to provide reasonable protection against accidental or inadvertent disclosure to outsiders." Jay Dratler, Jr., *Intellectual Property Law: Commercial, Creative and Industrial Property*, Vol. 1, § 4.03[3][a] (2003). As Professor Dratler has explained in his leading treatise:

> Although few judicial opinions elaborate these purposes, as distinguished from the policies underlying trade secret protection in general, three of them are readily apparent. First, the "reasonable efforts" requirement seeks to insure that employees and others are warned of the claim of secrecy, not just in anticipation of a lawsuit, but as a matter of ongoing commercial practice. In so doing, the "reasonable efforts" requirement helps reduce the risk that trade secret claims will be used as pretexts to suppress competition. Second, it reinforces the requirement for limited availability by making reasonably certain that the alleged trade secret is unlikely to become generally available to competitors through the owner's lapse or default. Finally, the "reasonable efforts" requirement recognizes the reasonable expectation of others that an owner of secrets of significant economic value will treat them as such. Thus, the law reduces the risk that those who reasonably rely on the absence of apparent protection will later be "sandbagged" by a lawsuit for misappropriation. In sum, the apparent purposes of the "reasonable efforts" requirement are to warn the trade secret owner's own personnel, to reduce the risk of inadvertent or

> accidental disclosure to a reasonable level, and to warn others who might have access to the trade secret and be tempted to use it without authorization. Accomplishing these modest purposes hardly requires absolute secrecy, but it is a worthy goal that the law should support.

Id. at § 4.03[3] (footnotes omitted).

Here, Wise combed InstallShield's ftp server on a daily basis downloading all new files that it had not already taken. PSAMF, ¶¶ 49-53. For example, from October 2 to October 9, 2002, the week in which Wise downloaded InstallShield's 103,000 Customer List and 6,000 Customer List, Wise combed InstallShield's ftp server every single day except Saturday and Sunday. PSAMF, ¶¶ 51, 67. In just one week, Wise downloaded 71 files using the confidential username and password of Jill Kawell 64 of 71 times. PSAMF, ¶¶ 51, 67. Plainly, the problem here is not a lack of notice to Wise. Rather, the problem here is that Wise used "electronic espionage," which constitutes "improper means" *per se* under Section 2(a) of the ITSA, 765 ILCS 1065/2(a) (defining "improper means" as including "electronic espionage"). *See also* Restatement (Third) of Unfair Competition, § 43, Cmt. (c) (trade secret acquired through burglary or wire tapping constitutes improper means).

D. The Cases Relied Upon by Wise Are Inapposite

None of the cases relied on by Wise granted summary judgment on the ground that an unsophisticated computer password constituted inadequate secrecy measures as a matter of law. Indeed, none of the cases relied upon by Wise involved computer passwords at all. Moreover, none of the cases relied upon by Wise were decided on summary judgment under the exacting *Rockwell Graphics* standards.

In *Jackson v. Hammer*, 274 Ill. App. 3d 59, 653 N.E. 2d 809, 210 Ill. Dec. 614 (4th Dist. 1995), the appellate court affirmed summary judgment on the basis that the plaintiff purchaser did not actually acquire the trade secret information in question, and therefore he could not claim misappropriation as to that information. *Lincoln Towers Insurance Agency v. Farrell*, 99 Ill. App. 3d 353, 425 N.E 2d 1034, 54 Ill. Dec. 817 (1st Dist 1981), which pre-dates the ITSA, contains little discussion of reasonable secrecy measures. Indeed, Lincoln Towers was decided on the basis that the plaintiff's customer list was generally known or least readily ascertainable.

Cincinnati Tool Steel Co. v. Breeds, 136 Ill. App. 3d 267, 482 N.E. 2d 1070, 90 Ill. Dec. 463 (2d Dist. 1985), which also pre-dates the ITSA, involved an interlocutory appeal from the denial of a preliminary injunction. The appellate court chose not to disturb the trial court's finding, made after the trial court assessed the credibility of the witnesses at the preliminary injunction hearing, that the plaintiff did not bear its burden of proof on its trade secret claim. The appellate court noted that in determining whether a customer list is a trade secret under the common law, it is significant "whether the information regarding the plaintiff's customers was kept under lock and key; in other words, whether the information was treated as confidential and secret by plaintiff." *Id.* at 177. The court in *Cincinnati Tool,* however, also emphasized that "the failure to keep [a trade secret] 'under lock and key' does not establish that the information was not confidential." *Id.* at 177, *citing Lawter International, Inc. v. Carroll*, 116 Ill. App. 3d 717, 451 N.E. 2d 1338, 72 Ill. Dec. 15 (1st Dist. 1983).

Finally, Wise's reliance upon *Religious Technology Center v. Lerma*, 897 F. Supp. 260 (E.D. VA. 1995), is also misplaced. In that case, the district court denied the plaintiff's motion for a preliminary injunction on the basis that the plaintiff could not show the claimed trade secrets were "not generally known." *Id.* at 266. The court in *Lerma* did not decide whether the plaintiff's secrecy efforts were reasonable under the circumstances. Rather, it found that the alleged trade secrets had been widely disseminated on the Internet, that the alleged trade secrets were in possession of the Washington Post, that the alleged trade secrets were publicly available in a federal court file in the Central District of California, and that the defendant was not "the only source of [the alleged trade secrets] on the Internet." *Id.* at 265-66.

VI. CONCLUSION

For these reasons, plaintiff requests that the Court deny defendant's motion for partial summary judgment.

Dated: November 21, 2003.

Respectfully submitted

Hillary P Krantz

One of the Attorneys for Plaintiff,
Installation Software Technologies,
d/b/a Installshield Software Corporation

William Lynch Schaller
John M. Murphy
Charles R. Topping
Hillary P. Krantz
BAKER & McKENZIE
One Prudential Plaza
130 East Randolph Drive
Chicago, IL 60601
(312) 861-8000
Firm ID: 28

CHIDOCS02, 608538.2

SEE CASE FILE FOR EXHIBITS